1. **Резюме по статье «Breaking RSA may not be equivalent to factoring»**

В статье говорится, что существуют 2 давние проблемы, чтобы доказать или опровергнуть, что взломать систему RSA, также сложно, как разложить на множители целые числа и что взломать протокол Диффи-Хеллмана так же сложно, как вычислить дискретный логарифм.

В статье дается опровержение утверждению, что взлом LE-RSA (RSA с низким показателем) эквивалентен факторизации. В статье приводятся доказательства тому, что нарушение алгоритма на самом деле может быть гораздо проще.

В исследовании используются прямолинейные программы (SLP) для многочленов. SLP для многочлена представляет собой последовательность многочленов такая что и для всех многочлен является либо равен 1, либо переменной или , где и .

Далее определяется понятие прямолинейного сокращения от факторизации к нарушению LE-RSA. RSA-SLP – алгебраическая схема, в которой элементы выполняют арифметические операции, а также извлекают корни e.

Прямолинейное сокращение – это рандомизированный алгоритм A, который на входе получает n, а на выходе набор RSA-SLP . Обозначим выходной набор значением . Для не пренебрежимо-малой части множество должно соответствовать N (с вероятностью, как минимум над случайными битами A).

Был сделан вывод, что факторизация не сводится к разбиению LE-RSA с использованием прямолинейных сокращений, за исключением простой факторизации.

Как результат исследования было введено 2 теоремы:

**Теорема 3.3.**

Предположим, что существует прямолинейное сокращение A, время работы которого равно . Далее предположим, что каждый RSA-SLP, сгенерированный при помощи A на входе содержит не более радикальных шагов. Тогда существует реальный алгоритм разложения на множители B, время выполнения которого равно и он факторизует все , которые сделал A.

Существуют более общие класс сокращения – алгебраические.

Алгебраическое сокращение А преобразует элемент при помощи специального оракула O. Время от времени A останавливается и предоставляет RSA-ALP для O. Затем оракул говорит «да» или «нет» в зависимости от того, равен ли RSA-SLP нулю в . В конечном счете А останавливается и выводит набор RSA-SLP , один из которых умножает N с вероятностью не менее (по случайным битам А).

Алгебраическое сокращение может быть преобразовано в реальный алгоритм разложения на множители.

**Теорема 3.7.**

Предположим, существует алгоритм алгебраического разложения на множители А, время выполнения которого равно . Далее предположим, что каждый из RSA-SLP сгенерированных при помощи A на входе содержит не более радикальных шагов. Тогда существует реальный алгоритм разложения на множители B, время выполнения которого равно и он факторизует все , которые сделал A.

Подчеркивается, что результат исследования не указывает на какую-либо слабость системы RSA. Вместо этого он представляет некоторые доказательства того, что взлом LE-RSA может быть проще факторизации. Однако ничто в этой работе не оспаривает того, что это, вероятно, всё равно будет трудноразрешимой задачей.